CONTRIBUIÇÃO PARA APLICAÇÃO DA GESTÃO DE RISCOS À PROTEÇÃO DE DADOS PESSOAIS PELA LGPD[1] NO ÂMBITO DA PGM[2]

Residente: Flávia Angelica Abrantes Russo[3]

Orientadora (Supervisora): Carolina Biella (Procuradoria Geral do Município)[4]

Avaliador: Huno Molina Rodrigues dos Santos (Procuradoria Geral do Município)[5]

RESUMO

A estrutura do processo de gestão de riscos pela metodologia proposta pela Controladoria Geral do Município para a Prefeitura de São Paulo é centrada em governança. A Procuradoria Geral do Município (PGM), órgão jurídico da Administração Pública Municipal Direta, tem se preparado desde 2021 para o atendimento à conformidade com a Meta 120 do Programa de Metas 2025 – 2028. Aplicam-se pela Administração Pública às premissas à proteção de dados pessoais pela LGPD o princípio da legalidade, o da supremacia do interesse público sobre o interesse privado, e o da publicidade, além de se realizar a avaliação de riscos exclusivamente por impacto em conformidade. A proposta de melhoria ao andamento do processo de gestão de riscos à proteção de dados pessoais pela LGPD na PGM fortalece governança.

Palavras-chave: gestão de riscos; LGPD; Administração Municipal; impacto de conformidade; proposta de melhoria.

---

[1] Lei Geral de Proteção de Dados (BRASIL, 2018).

[2] Procuradoria Geral do Município de São Paulo.

[3] Residente em Gestão Pública na Procuradoria Geral do Município. Especialista em Gestão em Energias Renováveis (Departamento de Economia Rural e Extensão - UFPR). Especialista em Engenharia de Saneamento Urbano e Rural (FSP-USP). Engenheira Química (EPUSP).

[4] Procuradora Coordenadora do Núcleo de Inovação e Tecnologia da Procuradoria Geral do Município de São Paulo.

[5] Procurador Atuante no Núcleo de Inovação e Tecnologia da Procuradoria Geral do Município de São Paulo.

São Paulo
Emissão original: 22 de abril de 2025
Revisão 01: 16 de junho de 2025
Publicação: 23 de junho de 2025

1. INTRODUÇÃO

O Programa de Metas (PdM) para o quadriênio de 2025 a 2028, em sua Versão Inicial, publicada em 1º de abril de 2025, apresenta como a Meta 120, a ser cumprida pela Controladoria Geral do Município (CGM): “garantir a proteção dos dados pessoais na administração municipal em conformidade plena com a Lei Geral de Proteção de Dados Pessoais (LGPD), por meio de 7 (sete) ações estratégicas”, entre as quais citam-se as seguintes:

- o lançamento de metodologia de diagnóstico de maturidade em privacidade e proteção de dados pessoais; e
- a condução, junto aos órgãos, de ciclos anuais de autoavaliação do diagnóstico de maturidade (SÃO PAULO [CIDADE], 2025).

O Decreto Municipal 59.767, de 15 de setembro de 2020, que regulamenta, no âmbito da Administração Municipal direta e indireta, a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), sancionada em agosto de 2021, dispõe, em seu artigo 2º, Inciso XIII, sobre o plano de adequação:

> Art. 2º Para os fins deste decreto, considera-se:
> (...)
> XIII - plano de adequação: conjunto das regras de boas práticas e de governança de dados pessoais que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos relacionados ao tratamento de dados pessoais (SÃO PAULO [CIDADE], 2020).

Em consonância às ações estratégicas da Meta 120 e em decorrência ao artigo 2º, Inciso XIII, do Decreto Municipal 59.767/2020, a CGM propôs um modelo de planejamento para elaboração do Programa de Governança em Privacidade e Proteção de Dados Pessoais.

Adicionalmente, a Instrução Normativa IN CGM/SP nº 02, de 23 de dezembro de 2024, aprova a metodologia de diagnóstico de maturidade em proteção de dados

pessoais e disciplina o procedimento de autoavaliação por parte dos órgãos da Administração Pública Municipal (SÃO PAULO [CIDADE], 2024).

Por meio da metodologia e do procedimento previstos na IN CGM/SP nº 02/2024, são estabelecidos 70 controles[6] organizados em oito temas, a saber, estrutura organizacional, governança, tratamento de dados pessoais, direitos dos titulares, resposta a incidentes, transparência, segurança da Informação, e gestão de terceiros, e distribuídos em cinco fases de verificação: preparatória, básica, intermediária, avançada e institucional.

A Procuradoria Geral do Município (PGM), órgão jurídico da Administração Pública Municipal Direta, tem se preparado desde 2021 para o atendimento à conformidade com a Meta 120 do PdM.

Atualmente, os controles “planejamento” e “plano de gestão de riscos”, que se localizam no tema governança, respectivamente, na fase preparatória e na fase básica do procedimento de autoavaliação supracitado, estão em desenvolvimento pelo Núcleo de Inovação e Tecnologia (NIT) da PGM para serem aplicados neste órgão.

1.1. OBJETIVOS

1.1.1. Objetivo Geral

O objetivo geral do presente trabalho é propor uma contribuição para a aplicação do processo de gestão de riscos à proteção de dados pessoais pela LGPD no âmbito da PGM.

[6] Os controles estabelecidos por meio da metodologia aprovada na IN CGM/SP nº 02/2024 são controles internos, i.e., realizados pelo próprio Poder Público, por seus agentes na Prefeitura de São Paulo e relacionados a requisitos da LGPD e boas práticas em proteção de dados pessoais.

1.1.2. Objetivos Específicos

Como pontos estruturantes do objetivo geral, os objetivos específicos são:

- apresentar a estrutura do plano de gestão de riscos aplicada à PGM;
- considerar as premissas à proteção de dados pessoais pela LGPD na aplicação pelo Poder Público no contexto da PGM;
- apresentar a situação de atendimento aos controles do Programa de Governança em Privacidade e Proteção de Dados Pessoais na PGM;
- analisar os controles internos realizados na PGM, face ao atendimento ao método de gestão de riscos; e
- propor recomendações para o andamento do processo de gestão de riscos à proteção de dados pessoais pela LGPD na PGM.

2. DESENVOLVIMENTO

2.1. ESTRUTURA DO PLANO DE GESTÃO DE RISCOS APLICADA À PGM

O Guia Orientativo de Diagnóstico de Maturidade em Proteção de Dados Pessoais da Prefeitura do Município de São Paulo identifica no tema governança (tema 02) controles que estabelecem uma sequência de atendimento, da fase preparatória à de institucionalização, do órgão da administração pública à gestão de riscos (CGM, 2025).

Essa sequência, centrada em governança, é composta por sete controles internos de proteção, sendo estes os identificados com os números 04 (na fase preparatória), 18 e 19 (na fase básica), 33 e 34 (na fase intermediária), 46 (na fase avançada), e 57 (na fase de institucionalização), que, para serem planejados, executados, monitorados ou avaliados, devem contar com a realização de controles

previstos em suas fases antecessoras, considerados os demais temas, além de governança.

Assim, o tema governança norteia o que e como se proceder, em linhas gerais, à execução de controles que devem estar concluídos nos demais temas (estrutura organizacional, tratamento de dados pessoais, direitos dos titulares, resposta a incidentes, transparência, segurança de informação e gestão de terceiros) em sua fase imediatamente antecessora para a execução de um controle de governança numa fase em andamento. Este tema, no modo como se apresenta, segundo a metodologia aprovada em dezembro de 2024 (SÃO PAULO [CIDADE], 2024), organiza o encadeamento de ações de execução de controles, como um todo.

Adicionalmente, a organização por governança reflete o Modelo das Três Linhas do IIA[7] 2020 (*The IIA*, 2020), adotado pela CGM como a estrutura de gestão de riscos proposta para aplicação às Unidades da Prefeitura de São Paulo (CGM, 2024).

Figura 1 – Estrutura de Gestão de Riscos aplicada às Unidades da Prefeitura de São Paulo (CGM, 2024).

[7] *The IIA* (*The Institute of Internal Auditors)*, Instituto de Auditores Internos do Brasil. O modelo citado é o de Três Linhas de Defesa 2020, visando à governança para ser utilizado em gerenciamento de riscos e controle organizacional.

O controle interno “plano de gestão de riscos” corresponde ao identificado como o número 18, dentre os 70 controles apresentados na metodologia de diagnóstico de maturidade em proteção de dados pessoais da Prefeitura do Município de São Paulo (CGM, 2025).

Os controles predecessores ao “plano de gestão de riscos”, com sua identificação de número e controle e situação de andamento realizado na PGM, são apresentados na Tabela 1 e na Tabela 2.

As colunas “controle” e “etapa do processo de gestão de riscos”, presentes nas Tabelas 1 e 2, informam quais controles devem ser cumpridos para se compor uma etapa deste processo, de acordo com a IN CGM/SP nº 01/2022 e o Manual de Gestão de Riscos elaborado pela CGM (SÃO PAULO [CIDADE], 2022; CGM, 2024).

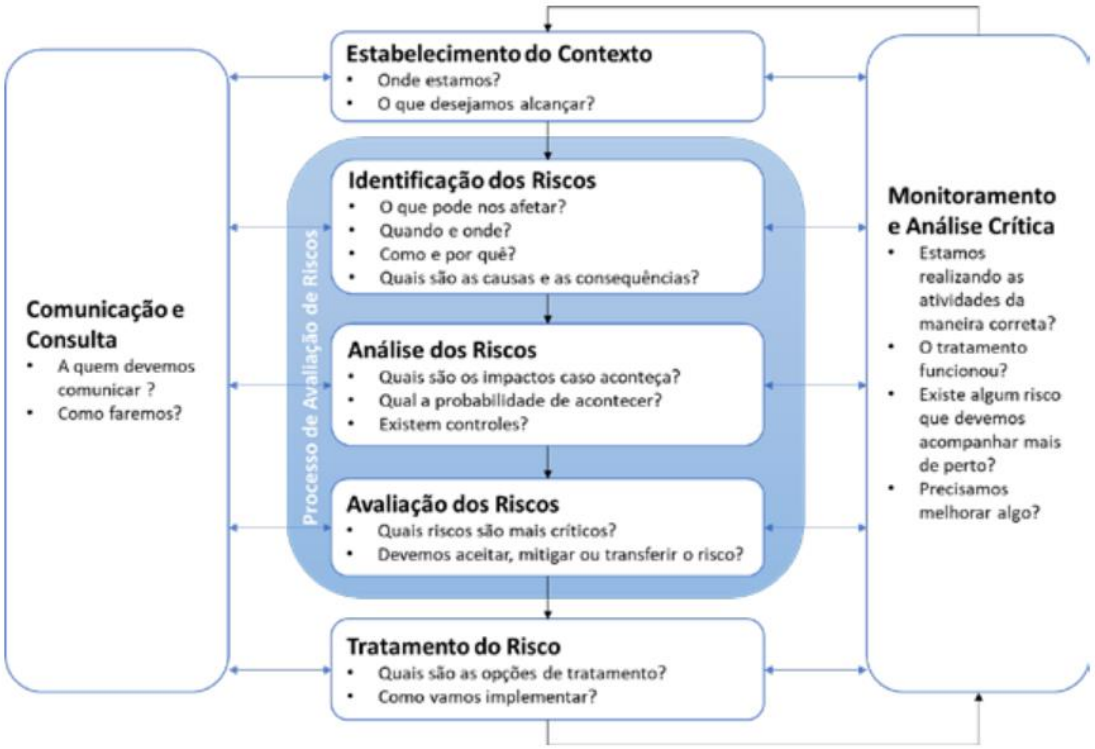

Figura 2 – Fluxograma do Processo de Gestão de Riscos (CGM, 2024).

O Processo de Gestão de Riscos adotado como metodologia (CGM, 2024) está baseado em modelos de processos constantes das normas ABNT NBR ISO 31.000:2018 e AS/NZS 4360:2004.

O ponto de partida do processo de gestão de riscos é o estabelecimento de contexto, e cada Unidade na Prefeitura de São Paulo deve estruturar o mapeamento de dados pessoais, bem como o mapeamento de processos que o precede, considerando o contexto de seu ambiente de atuação (interno e externo), porque a peculiaridade de cada contexto (em cada Unidade) implica "diferentes riscos e diferentes gradações de riscos à segurança da informação, à privacidade e à proteção de dados pessoais" (SÃO PAULO [CIDADE], 2023).

"Risco é a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos" (CGM, 2024, p. 18).

Assim, considerando-se a aplicação da proteção de dados pessoais pela LGPD no contexto da PGM:

- No estabelecimento deste contexto, cabe ao Núcleo Especializado de Gestão de Riscos (segunda linha na estrutura de gestão de riscos, Figura 1) ter clareza sobre quais os objetivos da PGM, comunicando-os formalmente, por meio do controle interno 03 (sensibilização) aos grupos de trabalho envolvidos no processo de gestão de riscos (na segunda linha e principalmente na primeira linha da estrutura, Figura 1); e

- Na etapa de identificação de riscos (fluxograma, Figura 2) os eventos a serem analisados são os que se enquadram como desvios dos objetivos da PGM, e, mapeados os processos, igualmente os que se configuram como desvios (de processos) nesse contexto.

Tabela 1: Identificação e Autoavaliação de Atendimento a Controles Predecessores (da Fase Preparatória) à Elaboração do Controle 18 “Plano de Gestão de Riscos” na PGM

Controle Predecessor (Número e Descrição)	Autoavaliação[8] PGM	Referência (Conformidade)	Etapa do Processo de Gestão de Riscos
01. Encarregado	Realizado	Art. 6º, X, Art. 23, III, LGPD	Estabelecimento e Análise de Contexto
02. Grupo de Trabalho	Realizado	Art. 6º, X, Art. 50, LGPD	Estabelecimento e Análise de Contexto
03. Sensibilização	Realizado	Art. 6º, X, Art. 50, LGPD Art. 14, VI, IN/CGM nº 01/2022	Estabelecimento e Análise de Contexto
04. Planejamento	Em andamento	Art. 6º, VIII, LGPD Art. 4º, III, Art. 15, Decreto nº 59.767/2020 Art. 13, I, Art. 14, I, IN/CGM nº 01/2022	Estabelecimento e Análise de Contexto
05. Mapeamento de Processos	Realizado	Art. 6º, VIII, LGPD Art. 4º, I, Decreto nº 59.767/2020 Art. 2º, Art. 14, IV, b, IN/CGM nº 01/2022	Estabelecimento e Análise de Contexto e Identificação de Riscos e Análise de Riscos
06. Mapeamento de Dados Pessoais	Realizado	Art. 6º, VIII, Art. 37, LGPD Art. 4º, I, Decreto nº 59.767/2020 Art. 2º, Art. 14, IV, IN/CGM nº 01/2022	Estabelecimento e Análise de Contexto e Identificação de Riscos e Análise de Riscos
07. Finalidades e Hipóteses Legais	Realizado	Art. 6º, I, II, III, Art. 23, I, LGPD Art. 10, Art. 14, IV, f, IN/CGM nº 01/2022	Estabelecimento e Análise de Contexto e Identificação de Riscos e Análise de Riscos
08. Canal de Atendimento aos Direitos dos Titulares	Realizado	Art. 6º, IV, Art. 17 a 20, LGPD Art. 6º, Decreto nº 59.767/2020	Identificação de Riscos e Análise de Riscos
09. Canal de Denúncias e/ou Notificações de Incidentes	Realizado	Art. 6º, X, Art. 48, Art. 50, § 2º, I, g, LGPD	Identificação de Riscos e Análise de Riscos
10. Informações do Encarregado	Realizado	Art. 6º, VI, Art. 41, § 1º, LGPD Art. 5º, parágrafo único, Decreto nº 59.767/2020	Identificação de Riscos e Análise de Riscos
11. Informações do Tratamento de Dados	Em andamento	Art. 6º, IV, VI, Art. 9º, I, II, Art. 23, I LGPD Art. 11, II, Decreto nº 59.767/2020 Art. 10, IN/CGM nº 01/2022	Identificação de Riscos e Análise de Riscos
12. Coleta de “Cookies”	Em andamento	Art. 6º, VI, Art. 9º, Art. 18, LGPD Art. 10, IN/CGM nº 01/2022	Identificação de Riscos e Análise de Riscos
13. Inventário de “Software” e de Ativos de Tecnologia da Informação	Realizado	Art. 6º, VII, Art. 46, Art. 47, Art. 49, LGPD, OT nº 004 e 013 do Decreto nº 57.653/2017	O controle 13 é uma boa prática, que pode ser demandada na etapa de Tratamento de Riscos (Figura 2).
14. Minutas Padrão	Em andamento	Art. 6º, VIII, Art. 33, II, b, Art. 39, LGPD Art. 114, III do Decreto nº 62.100/2022	O controle 14 é uma boa prática de tratamento de dados pessoais, que pode ser demandada na etapa de Tratamento de Riscos (Figura 2).
15. Mapeamento dos Contratos e Compartilhamentos	Não aplicável	Art. 6º, VIII, Art. 26, Art. 27, Art. 37, Art. 39, LGPD Art. 14, IV, j, k, l, IN/CGM nº 01/2022	Não aplicável no contexto da PGM

[8] Em 4 de abril de 2025.

Tabela 2: Identificação e Autoavaliação de Atendimento a Controles Predecessores (da Fase Básica) à Elaboração do Controle 18 “Plano de Gestão de Riscos” na PGM

Controle (Número e Descrição)	Autoavaliação[9] PGM	Referência (Conformidade)	Etapa do Processo de Gestão de Riscos
17. Capacitação do Grupo de Trabalho	Não iniciado	Art. 6º, X, Art. 50, LGPD Art. 13, III, IN/CGM nº 01/2022	Identificação de Riscos e Análise de Riscos
19. Política de Gestão de Riscos	Não iniciado	Art. 6º, VIII, Art. 50, LGPD Art. 4º, II, Decreto nº 59.767/2020 Art. 4º e 14, V, h, IN/CGM nº 01/2022	Identificação de Riscos e Análise de Riscos
21. Fluxo de atendimento	Não iniciado	Art. 6º, X, Art. 50, LGPD Art. 13, III, IN/CGM nº 01/2022	Identificação de Riscos e Análise de Riscos
22. Resposta às solicitações dos titulares	Não iniciado	Art. 6º, IV, Art. 19, II, Art. 23, § 3º, LGPD	Identificação de Riscos e Análise de Riscos
23. Fluxo de comunicação de incidentes	Não iniciado	Art. 6º, X, Art. 48, Art. 50, § 2º, I, g, LGPD	Identificação de Riscos e Análise de Riscos
24. Resposta aos incidentes	Não iniciado	Art. 6º, X, Art. 48, Art. 50, § 2º, I, g, LGPD	Identificação de Riscos e Análise de Riscos

[9] Em 4 abril de 2025.

2.2. PREMISSAS À PROTEÇÃO DE DADOS PESSOAIS PELA LGPD NA APLICAÇÃO PELO PODER PÚBLICO NO CONTEXTO DA PGM

Observam-se as seguintes premissas na aplicação da LGPD no contexto da PGM, com desdobramentos ao processo de gestão de riscos:

- Na avaliação dos riscos, a categoria de impacto, a qual se atribui valor ao se realizar o processo de gestão de riscos à proteção de dados pessoais aplicada à LGPD é exclusivamente a de conformidade, i.e., o impacto do risco é avaliado em função da abrangência (extensão e gravidade) do dano associado a descumprimentos de políticas e processos internos (da PGM), atos normativos municipais ou atos normativos estaduais e federais (CGM, 2024); e

- Os princípios da legalidade e da supremacia do interesse público sobre o interesse particular fundamentam atenuações na aplicação da LGPD, implicando no precedente para a retenção (permanente) dos dados (de pessoas físicas).

Adicionalmente, quanto a aspectos a serem analisados no processo de gestão de riscos à luz da LGPD, faz-se necessário identificar quais são os controles internos de segurança da informação relacionados à privacidade e à proteção de dados pessoais, dado que, embora sejam temas distintos, os controles de segurança de informação e de privacidade e proteção de dados são sinérgicos, havendo medidas e controles de segurança de informação essenciais para a garantia da privacidade e da proteção de dados pessoais (CGM, 2025).

Além disso, deve ser observado o princípio da publicidade no atendimento aos controles internos que zelam pela tratativa entre os titulares de dados (servidores públicos, contribuintes ou particulares) e o controlador, que é o Município de São Paulo (Art. 9º, I, II, Art. 23, I LGPD Art. 11, II, Decreto nº 59.767/2020, Art. 10, IN/CGM nº 01/2022).

2.3. SITUAÇÃO DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA PGM

A adequação da PGM à LGPD, estruturada pelo Programa de Governança em Privacidade e Proteção de Dados Pessoais, se encontra atualmente na conclusão da fase 01 (preparatória). Nesta fase está previsto o atendimento a 15 controles internos, sendo que um deles, o controle 04, em governança, é o controle de planejamento (do Programa).

A partir da Tabela 1 - Identificação e Autoavaliação de Atendimento a Controles Predecessores (da Fase Preparatória) à Elaboração do Controle 18 “Plano de Gestão de Riscos” na PGM – e da análise de informações contidas na planilha “PGM - IDP - Público” -- que se encontra, em 17 de abril de 2025, em preparação para ser publicada e, portanto, não será apresentada como um conteúdo de Anexo neste momento, e está atualizada até 10 de março de 2025 --, foram desenvolvidas as informações apresentadas na Tabela 3, para a etapa de contextualização, e, na Tabela 4, para a etapa de identificação e análise de riscos.

O diagnóstico situacional do Programa de Governança em Privacidade e Proteção de Dados Pessoais na PGM foi realizado com base em informações atualizadas e disponíveis em NIT até 17 de abril de 2025, às 10h30’.

O atendimento a evidências de realização de cada controle predecessor ao “plano de gestão de riscos” foi verificado comparando essas informações disponíveis em NIT com a pergunta verificadora ao cumprimento do controle (SÃO PAULO [CIDADE], 2022).

O trabalho atualmente no NIT, concentrado no atendimento aos 15 controles internos da fase preparatória e realização dos predecessores ao controle 18, “plano de gestão de riscos”, segue em andamento até 30 de abril de 2025 para consolidação de autoavaliação de maturidade pela PGM e apresentação à CGM, com execução de ações de melhoria contínua já nesta fase.

Tabela 3: Atendimento dos Controles Predecessores (da Fase Preparatória) à Etapa de Estabelecimento de Contexto do Processo de Gestão de Riscos

Controle Predecessor	Situação Baseada em Evidências	Análise de Evidências	Atendimento à Etapa de Contextualização
01. Encarregado	Realizado em 28/02/2025. https://capital.sp.gov.br/web/procuradoria_geral/w/links/369341	Atendido	Atendido
02. Grupo de Trabalho	Realizado em 27/02/2025. ORDEM INTERNA PGM/NIT N° 01/2025	Atendido com Ressalvas	Atendido com Recomendações
03. Sensibilização	Realizado em 19/07/2024 (e-mail), e de agosto a setembro de 2024 (CEJUR).	Atendido com Ressalvas	Atendido com Recomendações
04. Planejamento	Em andamento desde fevereiro de 2025.	Formalização de Acompanhamento de Planejamento em 4 de abril de 2025	Em andamento
05. Mapeamento de Processos	Planilha: ““PGM - IDP - Público”.	Parcialmente Atendido	Recomendações
06. Mapeamento de Dados Pessoais	Em andamento desde 2021, com coleta de dados e informações das áreas da PGM diretamente com essas áreas. A periodicidade de atualização dos dados e informações é a cada dois anos (tendo ocorrido em 2023 e em andamento neste ano desde fevereiro de 2025). Planilha ““PGM - IDP - Público”.	Atendido com Ressalvas	Atendido com Recomendações
07. Finalidades e Hipóteses Legais	Realizado	Não atendido	Recomendações

Tabela 4: Atendimento dos Controles Predecessores (da Fase Preparatória) à Etapa de Identificação e Análise de Riscos (IAR) do Processo de Gestão (de Riscos)

Controle	Situação Baseada em Evidências	Análise de Evidências	Atendimento à Etapa de IAR
08. Canal de Atendimento aos Direitos dos Titulares	Realizado em 28/02/2025. https://capital.sp.gov.br/web/procuradoria_geral/w/links/369341	Atendido	Atendido
09. Canal de Denúncias e/ou Notificações de Incidentes	Realizado em 28/02/2025. https://capital.sp.gov.br/web/procuradoria_geral/w/links/369341	Atendido	Atendido
10. Informações do Encarregado	Realizado em 28/02/2025. https://capital.sp.gov.br/web/procuradoria_geral/w/links/369341	Atendido	Atendido
11. Informações do Tratamento de Dados	Em revisão	Atendido com Ressalvas	Atendido com Recomendações
12. Coleta de Cookies	Em andamento	Em andamento	Em andamento
13. Inventário de Software e de Ativos de Tecnologia da Informação	Realizado	Atendido com Ressalvas	Aplicável à Etapa posterior à IAR
14. Minutas Padrão	Em andamento	Não atendido	Aplicável à Etapa posterior à IAR

2.4. ANÁLISE DOS CONTROLES INTERNOS (EM ANDAMENTO NA PGM), DE ACORDO COM O MÉTODO DE GESTÃO DE RISCOS

Das informações e dados apresentados nas Tabelas 1, 2, 3 e 4, a análise dos controles internos 02, 03, 05, 06, 07 e 11, frente à sua utilização no método para estabelecimento de contexto, identificação e análise de riscos é realizada no presente item 2.4.

São considerados controles internos em andamento na PGM os que foram realizados e atendidos com ressalvas, atendido parcialmente, ou não atendido, ou os que estão em desenvolvimento.

Nesta análise são considerados os controles internos que têm utilidade às etapas de identificação e análise de riscos (IAR), conteúdo do controle interno 18, plano de gestão de riscos, além de os controles internos que são necessários à etapa que precede a IAR, que se atém ao estabelecimento de contexto (Figura 2, item 2.1 do presente documento).

Além disso, esta análise foi realizada à luz das premissas que constam no item 2.2 do presente documento e considerando o Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública Municipal (CGM, 2024; CGM, 2025; SÃO PAULO [CIDADE], 2023).

Os controles 02, 03, 05, 06 e 07 devem ser resolvidos à etapa de contexto do processo de gestão de riscos. Além disso, observa-se que esses controles compõem a Fase Preparatória do Programa de Governança em Privacidade e Proteção de Dados Pessoais proposto pela CGM aos órgãos da Prefeitura de São Paulo. Assim, atender à Fase 01 do Programa é cumprir o estabelecimento de contexto do processo de gestão de riscos, sendo possível começar a adentrar à realização do controle interno 18 (SÃO PAULO [CIDADE], 2024; CGM, 2025; CGM, 2023).

A descrição da análise de evidências para os controles 02, 03, 05, 06 e 07, que estão em andamento na PGM e compõem a Fase Preparatória (01), é apresentada a seguir:

- Controle 02 (Grupo de Trabalho): este controle foi atendido com ressalvas,

porque não há evidências de que o Grupo de Trabalho conte com o apoio e/ou a participação da Alta Gestão. Justificativa para a análise: embora o Grupo de Trabalho tenha sido constituído por meio da ORDEM INTERNA PGM/NIT N° 01/2025 e realizado dentro das atribuições do NIT, por meio da Portaria PGM 22/2024, há proposta de melhoria a ser no item do 2.5 do presente documento em atendimento a boas práticas e a governança, de acordo com o Art. 50 da LGPD;

- Controle 03 (Sensibilização): este controle foi atendido com ressalvas. Justificativa para a análise: embora haja evidências apresentadas para o início de ações de sensibilização sobre o tema na PGM, não há evidências apresentadas sobre sua continuidade ou avaliação de mudança de comportamento sobre o tema na PGM, de modo sistêmico;

- Controle 05 (Mapeamento de Processos): este controle foi considerado parcialmente atendido. Justificativa para a análise: o mapeamento de processos apresentado identificou o que é cada processo de trabalho, mas não como ocorre o processo, sendo necessário verificar as atividades em cada processo levantado e por meio de quais tarefas se dá o tratamento de dados (Art. 6º, VIII, LGPD);

- Controle 06 (Mapeamento de Dados Pessoais): este controle foi considerado atendido com ressalvas. Justificativa para a análise: uma vez atendido o controle 05, o cumprimento do controle 06, com “as informações, de forma clara, adequada e ostensiva, sobre todo o ciclo de vida dos dados pessoais do titular” (CGM, 2025) na PGM acaba sendo uma decorrência. O atendimento ao controle 06 é necessário para funcionar como salvaguarda quando da etapa de tratamento de riscos do processo de gestão de riscos (Art. 6º, VIII, LGPD); e

- Controle 07 (Finalidades e Hipóteses Legais): este controle, considerada a evidência apresentada, foi considerado não atendido. Justificativa para a análise: não foram apresentadas evidências de atendimento ao Art. 6º, I, II, III, LGPD, e ao Art. 23, I, LGPD.

A descrição da análise de evidências para o controle 11, que está em revisão

na PGM e compõe a Fase Preparatória (01), é apresentada a seguir:

- Controle 11 (Informações do Tratamento de Dados): este controle foi considerado atendido com ressalvas e está atualmente em revisão na PGM. Justificativa para a análise: não foram apresentadas evidências de atendimento aos Art. 6º, IV, V, LGPD, Art. 9º, I, II, Art. 23, I LGPD Art. 11, II, Decreto nº 59.767/2020.

2.5. RECOMENDAÇÕES E PROPOSTA DE MELHORIA

As recomendações descritas a seguir derivam da análise apresentada sobre o desenvolvimento e situação dos controles internos predecessores ao controle 18, plano de gestão de riscos.

A proposta de melhoria visa ao desenvolvimento e cumprimento do controle 04 e ao prosseguimento do tema 02, governança, e se encontra em construção pelo NIT, com a colaboração de demais áreas da PGM e orientação, quando necessária, da CGM.

O controle 02 está abordado diretamente na proposta de melhoria.

As recomendações para os demais controles internos em andamento na PGM são as seguintes:

- Controle 03 (Sensibilização):
    - Realizar e/ou apresentar evidências sobre comunicação contínua para as áreas na PGM sobre conscientização à privacidade e à proteção de dados pessoais de titulares (servidores, contribuintes e particulares) pela LGPD;
    - Apresentar as evidências sobre a participação das áreas da PGM no treinamento assíncrono e “online” sobre o tema divulgado pelo CEJUR em 06 agosto de 2024; e

- Apresentar evidências sobre a avaliação de conhecimento retido pelos participantes desse treinamento divulgado pelo CEJUR.

- Controle 05 (Mapeamento de Processos):

  - A partir da identificação de processos realizada na planilha “PGM - IDP - Público”, realizar o mapeamento de fluxo de cada processo de trabalho identificado para que seja possível se verificarem os desvios de objetivo de cada etapa de processo ao se proceder à identificação e à análise de riscos, além de se analisar a suficiência de medidas de mitigação de riscos ou de se atribuir salvaguardas necessárias quando do tratamento de riscos.

- Controle 06 (Mapeamento de Dados Pessoais):

  - Verificar com a CGM a possibilidade de orientação para cumprimento do Art. 2º da IN CGM 01/2023:

> “Art. 2º O Mapeamento do Fluxo de Dados Pessoais tratados por cada unidade, previsto no artigo 4º, inciso I, do Decreto Municipal nº 59.767/2020, deverá observar o Anexo I – “Mapeamento de Dados Pessoais” e ser disponibilizado, centralizado, em plataforma única, a ser viabilizada pela Controladoria Geral do Município (CGM), com o apoio técnico e operacional da Secretaria Municipal de Inovação e Tecnologia (SMIT) e do Comitê Central de Governança de Dados, instituído pelo Decreto Municipal nº 60.663/2021, de modo a conter as informações, de forma clara, adequada e ostensiva, sobre todo o ciclo de vida dos dados pessoais do titular, com a indicação da unidade em que se localizam, bem como o status do processo ou atividade, caso necessário” (NR) (SÃO PAULO [CIDADE], 2023).

- Controle 07 (Finalidades e Hipóteses Legais):

  - Apresentar as evidências de atendimento ao Art. 6º, I, II, III, LGPD, e ao Art. 23, I, LGPD.

- Controle 11 (Informações do Tratamento de Dados):

  - Apresentar as evidências de atendimento ao Art. 6º, IV, V, LGPD, Art. 9º, I, II, Art. 23, I LGPD Art. 11, II, Decreto nº 59.767/2020; e

  - Na preparação de evidências que se encontram sob revisão no NIT,

nas informações sobre finalidade do tratamento na planilha “PGM - IDP - Público”, acrescentar informação sobre “previsão legal” nas células em que estiverem em branco, observando a aderência às informações sobre “hipótese de tratamento” nesta planilha.

O controle 02 está intrinsecamente ligado à estrutura de gestão de riscos (Figura 1), inspirada no Modelo das Três Linhas de Defesa, apresentado no item 2.1 (CGM, 2024).

Por essa estrutura, tem-se que:

- O Comitê de Gestão de Riscos deve ser indicado e formalizado pela Alta Gestão;

- O Núcleo Especializado de Gestão de Riscos deve ser coordenado pelo Responsável pelo Controle Interno (RCI) no órgão. Cabe a este Núcleo (segunda linha na estrutura de gestão de riscos, Figura 1) “a efetiva implementação da Gestão de Riscos” (CGM, 2024, p. 9); e

- “Os Gestores de Riscos usualmente são os gestores diretos dos servidores que executam as atividades relacionadas aos riscos” (CGM, 2024, p. 10).

Na PGM atualmente observam-se atribuições em NIT, que, de acordo com a estrutura de gestão de riscos proposta (CGM, 2024), podem ser responsabilidade principalmente do Núcleo Especializado de Gestão de Riscos.

Além disso, considerando-se que o Grupo de Trabalho estabelecido em atendimento ao controle interno 02 está com a responsabilidade de zelar pelo cumprimento dos 70 controles que perfazem o Programa de Privacidade e Proteção a Dados Pessoais na PGM, conforme o andamento das fases do programa for ocorrendo, serão observadas responsabilidades de Gestores de Riscos e do Comitê de Gestão de Riscos podendo ser atribuídas a este Grupo de Trabalho em NIT.

Assim, para poder se garantir governança no processo de gestão de riscos na PGM, que é o tema que norteia a estrutura programática do modelo (com os 70 controles), propõe-se, como melhoria, que:

- O Comitê de Gestão de Riscos deve ser indicado e formalizado pelo Gabinete da PGM;

- O Núcleo Especializado de Gestão de Riscos deve ser coordenado pelo Responsável pelo Controle Interno (RCI) na PGM, sendo que a Controladoria Interna da PGM é a função institucional de sua Corregedoria;

- Os Gestores de Riscos devem ser os gestores diretos dos servidores que executam as atividades relacionadas aos riscos em cada processo de trabalho identificado na planilha “PGM - IDP - Público”; e

- A composição de cada equipe de atendimento ao processo de gestão de riscos (Comitê, Núcleo e Gestores) deve ser independente entre si quanto a responder por suas atribuições nesse processo.

3. CONCLUSÕES

Todas as premissas à privacidade e proteção de dados pessoais pela LGPD no contexto da PGM aplicadas ao processo de gestão de riscos se estendem aos demais órgãos e entidades da Prefeitura de São Paulo.

Embora haja a necessidade de se demonstrar por meio de evidências a realização de controles como sensibilização ao tema, observa-se no dia a dia da PGM, por meio reuniões, tarefas e atividades no NIT e/ou na interface com outras áreas, como CEJUR (Centro de Estudos Jurídicos) e AJC (Assessoria Jurídico Consultiva) um apreço pelo tema privacidade e proteção de dados pessoais, além de um interesse em se compreender e realizar mapeamento de processos com vista a tratamento de riscos.

As recomendações e a proposta de melhoria apresentadas visam a fortalecer governança no processo de gestão de riscos na PGM.

Agradecimentos aos colegas Ana Beatriz de Oliveira Santana (Secretaria Municipal de Desenvolvimento Econômico e Trabalho - SMDET), André Aparecido de Carvalho (SMDET), Bruno dos Santos Kobayashi (PGM), Carolina Biella (PGM), Davi Carlos de Jesus Filho (SMDET), Fabrício Augusto dos Santos Reis (Secretaria de Governo Municipal - SGM), Huno Molina Rodrigues dos Santos (PGM), Juraci Pereira Silva (PGM), Karina Sousa Dos Santos (SMDET), Lucas Abraão Hastings Dória Silva (Secretaria Municipal de Gestão - SEGES), Lucas Rossanez da Silva (SMDET), Maíra Cavalcanti Rocha (Secretaria Municipal de Assistência e Desenvolvimento Social - SMADS), Marcus Vinicius Marins (Controladoria Geral do Município - CGM), Murilo Barreto Almeida (PGM), Patrícia Estevam Holanda (PGM), Poliana Lisboa de Almeida (SMDET), Radomir Tomitch (SMDET) e Roberto Stefani Takahashi (SMDET), na Prefeitura de São Paulo, pelo apoio e incentivo no desenvolvimento técnico de temas aplicados ao dia a dia de nosso trabalho na gestão pública, e a **todos os Residentes da 2ª Turma** do Programa de Residência em Gestão Pública, bem como, na PGM, a toda equipe do Núcleo de Inovação e Tecnologia (da Coordenadoria Geral do Contencioso Judicial) e às equipes da Coordenadoria Geral de Gestão e Modernização e da Assessoria Jurídico Consultiva, da Coordenadoria Geral do Consultivo, e, na SEGES, à Coordenação Geral e todas as Divisões da Escola de Administração Pública de São Paulo. Na PGM (Edifício Matarazzo) agradeço também à equipe terceirizada prestadora de serviços de limpeza e zeladoria (Edifício Matarazzo), mantendo diariamente a harmonia e asseio do ambiente físico, bem como à equipe terceirizada prestadora de serviços de recepção e segurança pela simpatia e celeridade no atendimento, e, na SMDET (Edifício Grande São Paulo), agradeço igualmente à equipe terceirizada prestadora de serviços de segurança e vigilância por toda solicitude e tranquilidade proporcionadas, especialmente quando necessário ter estado em horários antes das 7h e após as 19h nesse edifício.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Norma Técnica ABNT NBR ISO 31000:2018. Gestão de Riscos** – Diretrizes. Rio de Janeiro: ABNT, 2018.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público**. 2ª edição. Brasília, DF, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 20 abr. 2025.

BRASIL. **Lei Federal nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, *Diário Oficial da União*, 15 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 25 mar. 2025.

BRASIL. **Lei Federal nº 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, *Diário Oficial da União*, 20 de dezembro de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm . Acesso em: 3 abr. 2025.

CONTROLADORIA GERAL DO MUNICÍPIO (CGM). **Guia Orientativo de Diagnóstico de Maturidade em Proteção de Dados Pessoais da Prefeitura do Município de São Paulo.** Disponível em: https://capital.sp.gov.br/documents/d/controladoria_geral/guia-orientativo-diagnostico-de-maturidade-cpd-cgm-pdf. Acesso em: 4 abr. 2025.

CONTROLADORIA GERAL DO MUNICÍPIO (CGM). **Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo.** Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/GuiaOrientativosobreaPrivacidadeeaProtecaodeDadosPessoaisparaaAdministracaoPublicadoMunicipiodeSaoPaulo_publicacao_26_01_2023.pdf. Acesso em: 7 abr. 2025.

CONTROLADORIA GERAL DO MUNICÍPIO (CGM). **Manual de Gestão de Riscos.** Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/Manual_Gestao_Riscos_versao01_2023_publicacao_03_01_2024.pdf. Acesso em: 7 abr. 2025.

CONTROLADORIA GERAL DO MUNICÍPIO (CGM). **Portaria PGM nº 49, de 27 de novembro de 2023.** Institui a Política de Gestão de Riscos da Controladoria Geral do Município de São Paulo. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/portaria-controladoria-geral-do-municipio-cgm-49-de-27-de-novembro-de-2023. Acesso em: 14 abr. 2025.

PROCURADORIA GERAL DO MUNICÍPIO (PGM). **Portaria PGM nº 22, de 22 de fevereiro de 2024.** Dispõe sobre a estrutura e as atribuições do Núcleo de Inovação e Tecnologia (NIT) da Procuradoria Geral do Município e dá outras providências. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/portaria-procuradoria-geral-do-municipio-pgm-22-de-22-de-fevereiro-de-2024. Acesso em: 16 abr. 2025.

QSP - CENTRO DA QUALIDADE, SEGURANÇA E PRODUTIVIDADE PARA O BRASIL E AMÉRICA LATINA. **Gestão de Riscos** – A norma AS/NZS 4360:2004. 2a edição. São Paulo: Risk Tecnologia Editora Ltda., 2004.

SÃO PAULO (CIDADE). **Decreto Municipal nº 59.767, de 15 de setembro de 2020.** Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta. São Paulo, *Diário Oficial da Cidade de São Paulo*, 15 de setembro de 2020. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020. Acesso em: 7 abr. 2025.

SÃO PAULO (CIDADE). **Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública Municipal.** Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/GuiaOrientativosobreaInstrucaoNormativaCGM-SPn%C2%BA01-2022paraaAdministracaoPublicadoMunicipiodeSaoPaulo_publicacao_26_01_2023.pdf. Acesso em: 26 mar. 2025.

SÃO PAULO (CIDADE). **Instrução Normativa CGM/SP nº 01/2022, de 21 de julho de 2022.** Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. São Paulo, *Diário Oficial da Cidade de São Paulo*, 22 de julho de 2022. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/instrucao-normativa-controladoria-geral-do-municipio-cgm-1-de-21-de-julho-de-2022. Acesso em: 26 mar. 2025.

SÃO PAULO (CIDADE). **Instrução Normativa CGM/SP nº 01/2023, de 13 de janeiro de 2023.** Altera a Instrução Normativa Controladoria Geral do Município – CGM nº 01, de 21 de julho de 2022, que estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. Disponível em: http://legislacao.prefeitura.sp.gov.br/leis/instrucao-normativa-controladoria-geral-do-municipio-cgm-1-de-13-de-janeiro-de-2023 . Acesso em: 21 abr. 2025.

SÃO PAULO (CIDADE). **Instrução Normativa CGM/SP nº 02/2024, de 23 de dezembro de 2024.** Aprova a Metodologia de Diagnóstico de Maturidade em Proteção de Dados Pessoais e disciplina o procedimento de autoavaliação por parte dos órgãos da Administração Pública Municipal. São Paulo, *Diário Oficial da Cidade de São Paulo*, 27 de dezembro de 2024. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/instrucao-normativa-controladoria-geral-do-municipio-cgm-2-de-23-de-dezembro-de-2024. Acesso em: 7 abr. 2025.

SÃO PAULO (CIDADE). **Programa de Metas 2025 - 2028.** Versão Inicial. São Paulo, SP, 2025. Disponível em: https://capital.sp.gov.br/documents/d/prefeitura%20de-sao-paulo/pdm_25_28-pdf. Acesso em: 1 abr. 2025.

THE INSTITUTE OF INTERNAL AUDITORS (IIA). **Modelo das Três Linhas do IIA 2020** – Uma Atualização das Três Linhas de Defesa, julho de 2020. Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20072020131817.pdf. Acesso em: 7 abr. 2025.